UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

Banco del Austro, S.A.,

Plaintiff, Case No. 1:16-cv-00628 (LAK)

v.

Wells Fargo Bank, N.A.,

Defendant.
----------x

PLAINTIFF BANCO DEL AUSTRO, S.A.'S MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT WELLS FARGO BANK, N.A.'S MOTION TO DISMISS THE COMPLAINT PURSUANT TO FRCP 12(b)(6)

Carlos A. Nunez-Vivas (*pro hac vice*)
can@wnflaw.com
Daniel Foodman (*pro hac vice*)
df@wnflaw.com
John G. Marfoe (*pro hac vice*)
jgm@wnflaw.com
WNF LAW, P.L. -
WASERSTEIN, NUNEZ & FOODMAN
1111 Brickell Avenue, Suite 2200
Miami, Florida 33131
(305) 760-8500

Attorneys for Plaintiff Banco Del Austro, S.A.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

I. STATEMENT OF FACTS

On February 2, 2011, Plaintiff BDA, an Ecuadorean bank, entered into a correspondent banking relationship with WFB, a domestic bank. Both signed an agreement entitled "Terms and Conditions for Global Financial Institutions" (the "Agreement"), which is attached to the Complaint as Exhibit "A" Ex. [1].[1] Consequently, WFB established BDA's correspondent account with WFB (hereinafter, the "Correspondent Account").

Pursuant to the Agreement drafted by WFB, BDA agreed to pay correspondent banking fees to WFB, and WFB agreed to service BDA's Correspondent Account. Among other things, WFB promised to verify the authenticity of SWIFT payment orders pursuant to a security procedure, which would be the SWIFT Authentication procedures in accordance with the SWIFT User Handbook. Agreement ¶ 3.1. In addition, WFB expressly agreed to comply with, as contract terms, all Laws of the United States, including the USA PATRIOT Act[2], regulations of the United States Treasury, and general US commercial banking practices. Agreement ¶¶ 7.7 and 7.8. In doing so, WFB agreed to implement and use a customer-centric fraud detection program that would take into account the type, purpose and anticipated activity of the Correspondent Account to detect unusual activity, report, and block/reject unusual activity. Accordingly, WFB's promise to comply with the Laws of the United States, including the USA PATRIOT Act, regulations of the United States Treasury, and general US commercial banking practices as part and parcel of its contractual obligations further restricted WFB's acceptance of payment orders issued in the name of BDA. Complaint ¶¶ 12-21.

---

[1] Exhibits are attached to the Declaration of John G. Marfoe, submitted herewith. All references to "Ex. [#]" are to exhibits to the Declaration of John G. Marfoe.

[2] The USA PATRIOT Act is formally known as "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001," which amended the Bank Secrecy Act, 31 U.S.C. § 5318

The significance of WFB's promise to comply with these laws and regulations ***as contract terms*** cannot be overstated. WFB's promise was a huge inducement for BDA, a foreign bank, to enter into a correspondent relationship with WFB. The promise provided further contractual assurances of layered security for BDA.[3] Complaint ¶¶ 11-13, 15-17 and 18.

On July 31, 2014, WFB notified BDA in writing of WFB's financial crimes risk management program ("Global FCRM Program"), which was designed to comply with the various laws of the United States[4], including the Bank Secrecy Act, as amended by the USA PATRIOT Act, and thus with the terms and conditions of the Agreement. Complaint ¶ 14-15; Ex. [2]. WFB boasted that its Global FCRM Program had detective controls, which included identifying unusual activity; automated transaction monitoring; customer surveillance; investigating the unusual activities identified, and determining whether they are suspicious; monitoring customer activity, and applying predictive analytics for customer-centric, cross-channel fraud detection; screening, blocking, and rejecting transactions appropriately; and reporting these matters (along with other regulatory reporting requirements). *Id.*

In sum, WFB contractually assured BDA that it had a layered security program in place necessary to detect, investigate, and block or reject suspicious or fraudulent activity and to report them to BDA (along with other regulatory reporting requirements), which reporting would alert BDA of such anomalous activity and allow BDA to prevent any fraud. Based on WFB's assurances, BDA reasonably expected WFB to detect, investigate, block/reject, and report

---

[3] Although the SWIFT Authentication procedure would be used to verify whether BDA was the originator of a payment order, it could not be used to verify whether suspicious activity originating from BDA's SWIFT terminal was fraudulent (due to third-party hacking, as happened in this case) or in fact authorized by BDA (as both would show as "originating" from BDA). Complaint ¶ 20. Thus, additional layered controls would be necessary.

[4] WFB specifically represented that, through its Global FCRM Program, it managed financial crimes risks associated with, among other things, Bank Secrecy Act ("BSA"), Anti-Money Laundering ("AML"), and External Fraud.

anomalous activity in the Correspondent Account, which activity had the potential to materially impact BDA's Correspondent Account.

On January 21, 2015, it became clear that WFB had failed to comply with its contractual duties and statutory duties under Article 4-A of the Uniform Commercial Code. On that date, BDA reported to WFB that the latter made unauthorized debits from the Correspondent Account resulting from fraudulent transactions. Complaint ¶ 22. As a result, BDA issued fraud alerts through SWIFT to WFB for the following unauthorized transfers (the "Unauthorized Transfers"):

	Date	Time	Sender	Amount (US$)	Beneficiary	Beneficiary's Bank	City
1.	1/12/2015	7:24 pm	Marina Breeze	$986,256.88	Mester Trading Corp.	HSBC	Hong Kong
2.	1/12/2015	7:02 pm	Femar	$1,424,638.06	Regal Prosper Trading Limited	HSBC	Hong Kong
3.	1/13/2015	7:04 pm	Constrindec, S.A.	$1,236,578.45	Regal Prosper Trading Limited	HSBC	Hong Kong
4.	1/13/2015	9:16 pm	Econotrans Ecuador	$663,297.31	Regal Prosper Trading Limited	HSBC	Hong Kong
5.	1/13/2015	10:38 pm	Econotrans Ecuador	$96,325.23	Nectali Martinez Hernandez	JP Morgan Chase	New York
6.	1/14/2015	12:01 am	Audiolec	$1,485,230.89	Regal Prosper Trading Limited	HSBC	Hong Kong
7.	1/14/2015	11:51 pm	Constrindec, S.A.	$1,375,240.23	Regal Prosper Trading Limited	HSBC	Hong Kong

8.	1/14/2015	7:06 pm	Audiolec	$1,486,230.22	Jose Mariano Castillo	Wells Fargo	L.A.
9.	1/16/2015	6:29 pm	Cosmica	$1,056,780.56	Fratelli Investments Limited	Mashrebank PSC	Dubai
10.	1/20,2015	6:56 pm	Indisir	$298,223.15	No Beneficiary Identified	HSBC	Hong Kong
11.	1/20/2015	11:46 pm	Raslogec	$95,731.18	JGM Asia Telecom	Hang Seng Bank	Hong Kong
12.	1/21/2015	7:56 pm	Autoline	$1,968,230.25	Jiushun Group Co.	HSBC	Hong Kong
			TOTAL:	$12,172,762.41			

Complaint ¶ 23.[5] As promised, WFB's layered security, including its Global FCRM Program, should have flagged as unusual, suspect or anomalous the Unauthorized Transfers because they

[5] BDA discovered that for each of the Unauthorized Transfers, an unauthorized user, using the internet, hacked into BDA's computer system after hours using malware that allowed remote access, logged onto the SWIFT Network purporting to be BDA, and redirected transactions to new beneficiaries with new amounts. Complaint ¶ 31. For example, the unauthorized user changed the original January 13, 2015, payment order from Constrindec, S.A., by issuing, at 11:51 p.m., the payment order and changing the beneficiary from Miami-Dade Pump and Supply Co. in Miami, Florida, to Regal Proper Trading Limited in Hong Kong, and the amount from a mere $2,946.63 to a whopping $1,375,240.23. Unfortunately, this risk with SWIFT is nothing new, as technology has evolved, and hackers have gotten more sophisticated. Recently, as reported in the Wall Street Journal on March 22, 2016, hackers infiltrated a bank's SWIFT terminal to misappropriate $100 million. According to the article, "cybercriminals deployed hacking tools, including keylogger software that monitors strokes on a keyboard, to steal Bangladesh Bank's credentials for the Swift system, a closed network used by financial institutions to authorize financial transactions through secure messages." Syed Zain Al-Mahmood, *Hackers Lurked in Bangladesh Central Bank's Servers for Weeks*, THE WALL STREET JOURNAL, March 22, 2016. Another article in the New York Times dated February 14, 2015, reported that bank hackers stole millions via Malware. David E. Sanger and Nicole Perlroth, *Bank Hackers Steal Millions via Malware*, N.Y. TIMES, February 14, 2015. The New York Times reported that "in some cases, transfers were run through the system operated by the

were inconsistent with the normal activity in the Correspondent Account, and thus indicative of fraud. Complaint ¶ 25. Indeed, the Unauthorized Transfers exhibited the following unusual or anomalous characteristics:

a. Unusual times of day for the SWIFTs (given that all were outside normal operating hours of BDA's SWIFT payment orders[6]);

b. Unusual amounts;

c. Unusual beneficiaries in unusual geographic locations (nine out of the twelve transfers were to beneficiaries located in Hong Kong, a reputed money laundering hub[7]);

d. Unusual frequency of transfer (twelve in nine days, with the second, third and fourth transfers being to the same entity in Hong Kong within the span

---

Society for Worldwide Interbank Financial Telecommunication, or Swift, which banks use to transfer funds across borders. ***It has long been a target for hackers*** — and long been monitored by intelligence agencies." (emphasis added).

[6] WFB argued that there is nothing anomalous about the time when the payment orders were issued, given that "BDA itself notified Wells Fargo of the Unauthorized Transfers at approximately 11 p.m." Motion at p. 14. WFB confuses a payment order with a Fraud Alert. Authorized payment orders were sent during BDA's regular business hours. The unauthorized payment orders were sent after BDA's regular business hours. This is a huge red flag.

[7] According to the U.S. Department of State's website on Money Laundering and Financial Crimes (http://www.state.gov/j/inl/rls/nrcrpt/1999/928.htm):

> Hong Kong's status as a major financial center with an open and democratic society makes it attractive to money laundering activities. The combination of low taxes, modern financial services, flexible corporate laws and the absence of foreign exchange controls attract funds from across the globe, including those involving criminal proceeds. Narcotic trafficking is the major source of criminal proceeds laundered in Hong Kong. Organized crime groups based in Hong Kong dominate large portions of the Southeast Asian narcotics trade. Other sources of criminal proceeds include loan sharking, gambling, and financial crimes. Foreign sources of criminal proceeds are likewise sent to Hong Kong for laundering and Hong Kong serves as a major transit point in international money laundering schemes.

of a mere 26 hours for substantial sums of money); and

e. The *same* entity in Hong Kong receiving *substantial* funds from *multiple* customers of BDA within a mere 26-hour period (e.g., Regal Prosper Trading Limited receiving funds from three different customers of BDA).

Complaint ¶ 26.

In sum, the Unauthorized Transfers were made in unusual times of the day, in unusual amounts, to unusual beneficiaries in unusual geographic locations (ten of twelve, including the first four), and in an unusual frequencies. For example, three of the first four wires, in the substantial amounts of $1,424,638.06, $1,236,578.45 and $663,297.31, were created outside the normal operating business hours of BDA and its SWIFT system, were in high amounts, sent to the **same** entity ("Regal Prosper Trading Limited") in an unusual geographic location (Hong Kong, a reputed money laundering center), within the span of only 26 hours from **three** different customers of BDA. Complaint ¶ 27. WFB's promised layered security program should have flagged these payment orders as suspicious, anomalous and extraordinary.

Thus, WFB should have detected, investigated, blocked/rejected and reported to BDA the Unauthorized Transfers. WFB failed to do so.[8] As a result, BDA filed its Complaint, raising claims for breach of contract (Count I), breach of Article 4-A (Count II) and breach of the common law duty of care (Count III). WFB is liable for the Unauthorized Transfers because:

1) WFB violated section 4-A-204(1) of the Uniform Commercial Code, which requires that the receiving bank (i.e., WFB) bear the risk of loss of

[8] In contrast, on January 27, 2015, Citibank refunded the sum of $1,845,286.86 to BDA as a result of the fraud alert issued by BDA as to an unauthorized transfer to its correspondent account maintained at Citibank for the same amount. Complaint ¶ 33. WFB failed to do the same, as it was required to do so by law. Instead, WFB only made a partial refund of the Unauthorized Transfer in the amount of US$1,486,230.22 by refunding the sum of $958,700.27. Complaint ¶ 34.

any unauthorized funds transfers. In violation of the statute, WFB failed to refund the Unauthorized Transfers to BDA, as it was obligated to do because:

a. The Unauthorized Transfers were not authorized by BDA pursuant to section 4-A-202(1) of the Uniform Commercial Code;

b. The Unauthorized Transfers were not effective against BDA pursuant to section 4-A-202(2) because:

i. The SWIFT Authentication procedure, by itself, is not a commercially reasonable security procedure, as required by section 4-A-202(2)(a) of the Uniform Commercial Code;

ii. WFB cannot prove that it accepted the Unauthorized Transfers in compliance with other provisions in the Agreement, as required by section 4-A-202(2)(b) of the Uniform Commercial Code; or

iii. WFB cannot prove that it accepted the Unauthorized Transfers in good faith, as required by section 4-A-202(2)(b) of the Uniform Commercial Code;

2) WFB materially breached the Agreement by failing to comply with provisions in the Agreement requiring it to detect, investigate, block/reject and report to BDA the Unauthorized Transfers;

3) WFB should have known that the Unauthorized Transfers were fraudulent given their anomalous characteristics, thus breaching its common law duty of care imposed on banks;

4) Neither the breach of the duty of care nor the breach of the Agreement are preempted by Article 4-A, inasmuch as both in effect rely on the fact that WFB should have known that the Unauthorized Transfers were fraudulent given their anomalous nature. Moreover, the breach of the Agreement claim relies as well on higher standards agreed-upon by WFB, including WFB's promise to implement and use layered controls, including a customer-centric fraud detection program that would take into account the type, purpose and anticipated activity of the Correspondent Account to detect unusual activity, report, and block/reject unusual activity; and

5) The Agreement does not prohibit any claim for negligence against WFB. To the contrary, it provides for such a negligence claim in paragraph 2.3.

Accordingly, WFB's Motion to Dismiss (the "Motion") must be denied.

II. ARGUMENT

For a complaint to be sufficient, the claim asserted must be one that, in light of the factual allegations, is at least "plausible." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). It must allege facts that, accepted as true, would be sufficient to permit a reasonable inference that the defendant has engaged in culpable conduct: "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). In this case, BDA has met this standard.

A. WFB IS LIABLE FOR THE UNAUTHORIZED TRANSFERS PURSUANT TO ARTICLE 4-A

The claim under Count II of the Complaint is for breach of statutory duties under Article 4-A of the Uniform Commercial Code ("Article 4-A"). BDA specifically alleges that WFB has

failed to comply with section 4-A-204(1), which imposes liability on WFB for the unauthorized transfers. Complaint ¶¶ 64-5; *Patco Const. Co., Inc. v. People's United Bank*, 684 F.3d 197, 208 (1st Cir. 2012) ("Under Article 4A, a bank receiving a payment order ordinarily bears the risk of loss of any unauthorized funds transfer.").

Specifically, section 4-A-204(1) requires a receiving bank to refund any funds (plus interest) from a payment order that was not authorized by the customer under UCC § 4-A-202.[9] "The only remedy of Receiving Bank is to seek recovery from the person who received payment as beneficiary of the fraudulent order." UCC § 4-A-203 cmt. 2.

1. THE UNAUTHORIZED TRANSFERS WERE NOT AUTHORIZED BY BDA

BDA did not authorize the Unauthorized Transfers under section 4-A-202(1), which provides that:

> A payment order received by the receiving bank is the authorized order of the person identified as sender if that person authorized the order or is otherwise bound by it under the law of agency.

BDA alleged that it did not authorize the Unauthorized Transfers. Complaint ¶ 48. As alleged in the Complaint, an unauthorized user remotely accessed BDA's computer system after hours, logged onto the SWIFT network purporting to be BDA, and redirected transactions to new beneficiaries with new and significantly higher dollar amounts. Upon discovery of the fraud, BDA promptly informed its correspondent banks, including WFB. Complaint ¶¶ 31-2.

Moreover, BDA is not bound under the law of agency because the payment orders were transmitted electronically via SWIFT. Complaint ¶ 49; UCC § 4-A-203 cmt. 1 ("In a very large

[9] WFB is required to refund the Unauthorized Transfers because they were not authorized by BDA under section 4-A-202(1) and were not effective against BDA under section 4-A-202(2). Section 4-A-203 is not at issue. Citations to comments in section 4-A-203 are made because section 4-A-202 "is discussed in the Comment following Section 4A-203." UCC § 4-A-202 cmt.

percentage of cases covered by Article 4-A, transmission of the payment order is made electronically. The receiving bank may be required to act on the basis of a message that appears on a computer screen. Common law concepts of authority of agent to bind principal are not helpful. There is no way of determining the identity or the authority of the person who caused the message to be sent."). Accordingly, WFB cannot enforce the Unauthorized Transfers against BDA pursuant to UCC § 4-A-202(1).

2. THE UNAUTHORIZED TRANSFERS ARE NOT EFFECTIVE AGAINST BDA

Likewise, WFB cannot enforce the Unauthorized Transfers against BDA pursuant to UCC § 4-A-202(2). This section provides in pertinent part that:

> If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if
>
> (a) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders, **and**
>
> (b) the bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer.

UCC § 4-A-202(2) (emphasis added). The Unauthorized Transfers are not effective against BDA because (a) the security procedure is commercially unreasonable, (b) WFB failed to accept the Unauthorized Transfers in compliance with other applicable provisions in the written Agreement, and (c) WFB failed to accept the Unauthorized Transfers in good faith. Complaint ¶ 51.

a. THE SWIFT AUTHENTICATION PROCEDURE, ALONE, IS COMMERCIALLY UNREASONABLE

Section 4-A-202(3) provides in pertinent part that:

> Commercial reasonableness of a security procedure is a question of law to be determined by considering the wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated.

"The UCC explains that '[t]he burden of making available commercially reasonable security procedures is imposed on receiving banks because they generally determine what security procedures can be used and are in the best position to evaluate the efficacy of procedures offered to customers to combat fraud.'" *Patco Const. Co., Inc.*, 684 F.3d at 209. "It is reasonable to require large money center banks to make available state-of-the-art security procedures." UCC § 4-A-203 cmt. 4. Thus, WFB, a large money center bank, is required to make available a state-of-the-art security procedure. This it failed to do.

Among other things, the Agreement provided that for SWIFTs, the SWIFT Authentication procedures would be used only "to verify that [BDA] is the originator of a payment order[.]" Agreement ¶ 3.1. Thus, although the SWIFT Authentication procedure would be used to verify that BDA "originated" the payment order, it could not be used to verify whether suspicious activity originating from BDA's SWIFT terminal was fraudulent (due to third-party hacking, as happened in this case) or in fact authorized by BDA (as both would show as "originating" from BDA). Complaint ¶ 20. According to WFB, it applied the so-called security procedure by merely looking at BDA's "unique SWIFT BIC identification code [on the payment orders], confirming that they were authenticated pursuant to the Agreement …" Motion at p. 6. If that is all WFB did, it is ludicrous. It is unreasonable as a matter of law.

In *Patco Const. Co., Inc.*, the court held that the security procedure used to verify electronic funds transfers using the internet was commercially unreasonable. In reaching this conclusion, the court offered a strong foundation for analyzing the commercial reasonableness of

a security procedure. Clearly, a "bank's generic 'one-size-fits-all' approach to customers violates Article 4-A's instruction to take the customer's circumstances into account." *Patco Const. Co., Inc.*, 684 F.3d at 212. By merely looking at the bank's BIC identification code, WFB has improperly applied a "one-size-fits-all" approach with BDA. Obviously, for all SWIFTS from any bank, WFB would have to look at the BIC identification code. Given that it admits in its Motion that all it had to do was look at the BIC identification code, it is applying an improper "one-size-fits-all" approach to customers, in violation of Article 4-A.

WFB's improper approach is patently unreasonable when one takes into account the fact that "[s]ome of the main risks involved in Swift may come from hackers, increased dependence of banks on IT, Open Technologies, and increased electronic access by customers." Dan Zhu, *Security Controls in Inter-Bank Fund Transfer*, 3 J. ELEC. COMM. RESEARCH 15, 19 (2002). "Attacks on the system are possible by the following means: (1) Readily available sophisticated hacking tools, (2) Packet/Address spoofing; (3) Stealth diagnostics; (4) Sniffers, (5) Sweepers and (6) Backdoors." *Id.*; *see also* n. 5, *supra*.

In *Patco Const. Co., Inc.*, the customer sued the bank for accepting fraudulent payment orders. A subsequent investigation of the customer's computer network revealed a malware program. As a result, the unauthorized users were able to provide one of the employee's ID, password, and answers to the challenge questions. The fraudulent payment orders were "uncharacteristic;" monies were sent to individuals to whom the plaintiff had never before sent funds, for greater amounts than ordinary, and on unusual days (i.e., funds would ordinarily be transferred on Fridays, yet the unauthorized transfers took place over the course of several days). *Patco Const. Co., Inc.*, 684 F.3d at 204-5.

The customer argued that the security procedure employed by the bank was unreasonable. The court agreed. The security procedure assigned a unique company ID to the customer, each of the customer's authorized employees was assigned a personal user ID and password, and each user had personalized answers to three challenge questions. The agreement between the customer and the bank provided that the "password constitutes authentication of all transactions performed[.]" *Id.* at 200. Separately, the bank built a risk profile for each user by tracking the user's online activity. Then, it used the profile data to calculate a score for each transaction based on deviation from previous transactions to detect unusual transactions. The bank failed to monitor these scores, which were to be used to detect anomalous activity in the account. Instead, the bank required that all users answer the challenge questions for transactions exceeding $1, which increased the risk that the secured information could be obtained using malware as it would increase the frequency that the challenge questions would be asked. *Id.* at 211-2.

In deciding that the security procedure was unreasonable, the court took into account security features available throughout the banking industry. *Id.* at 200-4. The court stressed that the bank's personnel were not monitoring the risk scores, whereas other banks did have employees monitoring risk scores and verifying high-scoring transactions with the customer. *Id.* at 212. The court faulted the bank's failure to employ security measures as recommended by the 2005 FFIEC[10] guidelines for internet banking security procedures, especially given the warnings

[10] "FFIEC" stands for the Federal Financial Institutions Examination Council, which, in responding to increased online banking fraud, issued guidance titled "Authentication in an Internet Banking Environment." *See* Fed. Fin. Insts. Examination Council, Authentication in an Internet Banking Environment (Aug. 8, 2001), *available at* http://www.ffiec.gov/pdf/authentication_guidance.pdf (hereinafter "Guidance"). The Guidance was intended to aid financial institutions in "evaluating and implementing authentication systems and practices whether they are provided internally or by a service provider." *Patco Const. Co., Inc.*, 684 F.3d

in the industry about fraud using malware. *Id.* at 211. Thus, the court held that "by May 2009, when the fraud in this case occurred, it was commercially unreasonable for [the bank's] security system to trigger nothing more than what was triggered in the event of a perfectly ordinary transaction in response to high scores that were generated by the withdrawals from [the customer's] account." *Id.* at 213.

In our case, WFB admits in its Motion that it did not even bother to monitor the Correspondent Account for any anomalous activity and implement a procedure to further authenticate an anomalous payment order. These circumstances are worse than in *Patco Const. Co., Inc.* This is especially true given the fact that, on June 28, 2011, the FFIEC issued supplemental guidance on internet banking authentication titled "Supplement to Authentication in an Internet Banking Environment." *See* Fed. Fin. Insts. Examination Council, *Supplement to Authentication in an Internet Banking Environment* (Aug. 8, 2001), *available at* (https://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf) (hereinafter "FFIEC Supp."). In its supplement, the FFIEC provides that financial institutions should implement "layered security." FFIEC Supp. at 4. Effective layered controls include, but are not limited to, "fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response." *Id.* The FFIEC then goes on to state that financial institutions' layered security programs must contain "at a minimum" processes "designed to detect anomalies and effectively respond to suspicious or anomalous activity related to … initiation of electronic transactions involving the transfer of funds to other parties." *Id.* at 5. "[M]anual or automated transaction monitoring or anomaly

---

201 (citation omitted). The Guidance provides that "financial institutions should periodically ... [a]djust, as appropriate, their information security program in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information." *Id*.

detection and response could have prevented many of the fraud since ACH/wire transfers being originated by fraudsters were anomalous when compared with the customer's established patterns of behavior." *Id.* Thus, commercial reasonableness requires today that a bank implement a program that meets this requirement, at a minimum. Indeed, "[t]ransaction monitoring/anomaly detection software has been in use for a number of years." *Id.* at 10. It is industry standard.

Thus, as a matter of law, WFB's security procedure, if limited to the SWIFT Authentication procedure (as it claims), it is unreasonable as a matter of law. It has no transaction monitoring/anomaly detection software, which use is standard in the banking industry to detect fraud in customers' accounts.

b. WFB FAILED TO ACCEPT THE UNAUTHORIZED TRANSFERS IN GOOD FAITH AND IN COMPLIANCE WITH THE APPLICABLE PROVISIONS IN THE AGREEMENT

WFB erroneously assumes that mere compliance with the SWIFT Authentication procedures would be sufficient to shift the risk of loss to BDA. Section 4-A-202(2)(b) is clear that, in addition to complying with the agreed-upon Security Procedure, WFB had to process the payment orders in compliance with any other applicable provision in the Agreement, and must have accepted the payment orders in good faith. WFB failed on both counts.[11]

i. WFB FAILED TO ACCEPT THE UNAUTHORIZED TRANSFERS IN COMPLIANCE WITH APPLICABLE PROVISIONS IN THE AGREEMENT

WFB argued that it only had to comply with the SWIFT Authentication procedure and nothing else. It is mistaken. WFB failed to comply with other applicable provisions of the Agreement, as required by section 4-A-202(2)(b), which "also requires the bank [i.e., WFB] to

[11] The failure to comply with a commercially reasonable security procedure and other applicable provisions is a question of fact. *See* UCC § 4-A-203 cmt. 4.

prove that it complied with any agreement or instruction that restricts acceptance of payment orders issued in the name of the customer." UCC § 4-A-203 cmt. 3. "***Such limitations may be incorporated into the security procedure itself or they may be covered by a separate agreement or instruction***. In either case, the bank ***must*** comply with the limitations if the conditions stated in subsection (b) are met." *Id.* (emphasis added). In this case, further limitations were covered in separate paragraphs of the Agreement.

"New York contract law permits parties to incorporate by reference statutes ***as terms of their contracts***." *Flagg v. Yonkers Savings & Loan Assoc., F.A.*, 307 F. Supp. 2d 565, 583 (S.D.N.Y. 2004) (emphasis added). Statutes that are incorporated by reference as terms of a contract "are enforceable by a breach of contract action[.]" *Id.* Statutes may be "included as contract terms either explicitly as text or incorporated by reference." *Id.*

As an example, the court in *Flagg* relied on *Wells v. Chevy Chase Bank, F.S.B.*, 377 Md. 197, 832 A. 2d 812 (2003). In *Wells*, the credit-card agreement between the customer and the bank contained a section entitled "Governing Law," which referenced Subtitle 9 of the Commercial Law Article of the Maryland Code, and "applicable federal law." 377 Md. at 199. The issue was whether the bank breached the Cardholder Agreement by improperly amending it in violation of Subtitle 9. *Id.* at 200-1. Thus, the court had to address the issue of "whether or not the language of the contract specifying Subtitle 9 requires [the bank] to comply with the credit card amendment provisions of Subtitle 9." *Id.* at 225. The bank argued that the reference to Subtitle 9 in a "Governing Law" provision was insufficient to transform the statute into a private contract. *Id.* at 208. The court disagreed, "concluding that the parties incorporated by reference state statutes as contract terms when [the] credit card agreement's governing law provision provided that '[t]his Agreement is made in Maryland. It is governed by Subtitle 9 of Title 12 of

the Commercial Law Article of Maryland Annotated Code and applicable federal law.'" *Flagg*, 307 F. Supp. 2d at 584.

Another example is the case of *American Rock and Salt Co., LLC. v. Norfolk Southern Corp.*, 180 F. Supp. 2d 420 (W.D.N.Y. 2001). In *American Rock and Salt Co., LLC.*, a clause in a rail service contract between a salt manufacturer and a railroad provided that "shipments made under the terms of this Contract are subject to … government, AAR and carrier rules, regulations and provisions …" 180 F. Supp. 2d at 425. The salt manufacturer claimed that the railroad breached the rail service contract because it violated obligations as a common carrier under 49 U.S.C. § 11101(A) and 11121(A)(1) (the Interstate Commerce Act or "ICA"). *Id.* at 424. The railroad moved to dismiss based on its argument that there was "no express or implied cause of action under the ICA for breach of a private contract for rail services." *Id.* The court denied the motion to dismiss, ruling that the parties themselves can "contractually agree to be bound by particular statutory or regulatory duties by importing those duties into the contract itself." *Id.* at 425.

In this case, the Agreement drafted by WFB is even more explicit about incorporating by reference other statutory laws as contract terms. It expressly provided that:

> These Terms & Conditions will be governed by and construed in accordance with the Laws of the US and the State of New York, including (without limitation) Articles 3, 4, 4A and 5 of the Uniform Commercial Code, … which are all incorporated herein by reference and made a part hereof.

Agreement ¶ 7.7. Moreover, "WFB assured BDA that not only would the relationship be also governed by the laws of the State of New York, including Article 4-A of the Uniform Commercial Code, but also that WFB would comply with all Laws of the United States applicable to it, including the USA PATRIOT ACT, and general US commercial banking

practices." Agreement ¶¶ 7.7 and 7.8; Complaint ¶ 12.[12] Specifically, WFB, as part and parcel of the Agreement's terms and conditions, promised "to comply with all Laws of the US applicable to it in any of its locations, including without limitations the USA PATRIOT ACT, … [and] regulations of the United States Department of the Treasury[.]" Agreement ¶ 7.8.[13] Indeed, in exchange for WFB's compliance with the USA PATRIOT ACT and other US Laws applicable to it, BDA agreed that WFB "may require that [BDA] provide … information to [WFB] about … any entity … transacting payments … through Correspondent's Account[.]" *Id.* In addition, the Agreement specifically provided that "[a]ccounts provided in connection with these Terms and Conditions are also governed by … general US commercial bank practices applicable in connection with the Account and the Services."[14] Agreement ¶ 7.7. And, finally, the Agreement provided that WFB, "[u]pon reasonable notice to [BDA]," may "modify procedures or Services" and "amend the Terms and Conditions." Agreement at Part 1.

---

[12] While it is true that the USA PATRIOT Act and the Bank Secrecy Act do not directly afford a private cause of action in favor of a customer, it does not mean that a bank and its customer cannot agree to incorporate the statute as contract terms in their agreement.

[13] The significance of WFB's promise to comply with these laws and regulations cannot be overstated. The promise is a huge inducement for a bank like BDA to enter into a correspondent relationship with a domestic bank. The promise provides further assurances of security for the foreign bank. In its Motion, WFB claims that references to other laws "refer to Wells Fargo's effort 'to help the US government fight the funding of terrorism and money laundering activities,' which might as a result require it to 'obtain, verify, and record information that identifies each person who opens an account.'" Motion at p. 18. That is not the case. The quoted language chosen by WFB out of context is from a section entitled "USA PATRIOT Act Notice." It does not qualify or limit at all any of the language incorporating by reference US laws, including the language wherein WFB expressly agrees to comply with the USA PATRIOT Act and Treasury regulations. In addition, even if one assumes that WFB's contractual interpretation is reasonable (which it is not), it does not control, inasmuch as WFB drafted the Agreement. Thus, BDA's reasonable contractual interpretation governs. *Aukema v. Chesapeake Appalachia, LLC*, 904 F. Supp. 2d 199, 209 (N.D.N.Y. 2012) ("In the event of an ambiguity, a contract will be construed against its drafter since the drafter is responsible for any ambiguity.").

[14] Clearly, WFB failed to comply with, at a minimum, general US commercial banking practices, as discussed in the section concerning the unreasonableness of WFB's security procedure given that it lacked, at a minimum, transaction monitoring/anomaly detection software, which has been in use in the banking industry for years.

Section 312 of the USA PATRIOT Act, as implemented by the Department of the Treasury's regulations, requires:

> U.S. financial institutions to establish due diligence and, where necessary, enhanced due diligence, policies, procedures and controls reasonably designed to detect and report money laundering through correspondent accounts and private accounts established or maintained by U.S. financial institutions for non-U.S. persons.

31 C.F.R. Part 103. Specifically, Department of Treasury regulations implementing the USA PATRIOT Act provide in pertinent part that:

> **(a)** ***In general.*** A covered financial institution shall establish a due diligence program that includes appropriate, specific, risk-based, and, where necessary, enhanced policies, procedures, and controls that are reasonably designed to enable the covered financial institution to detect and report, on an ongoing basis, any known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered, or managed by such covered financial institution in the United States for a foreign financial institution. The due diligence program required by this section shall be a part of the anti-money laundering program otherwise required by this subpart. Such policies, procedures, and controls shall include:
>
> **(1)** Determining whether any such correspondent account is subject to paragraph (b) of this section;
>
> **(2)** Assessing the money laundering risk presented by such correspondent account, based on a consideration of all relevant factors, which shall include, as appropriate:
>
> **(i)** The nature of the foreign financial institution's business and the markets it serves;
>
> **(ii)** The ***type, purpose, and anticipated activity*** of such correspondent account;
>
> * * *
>
> **(3)** Applying risk-based procedures and controls to each such correspondent account reasonably designed to detect and report known or suspected money laundering activity, including a periodic review of the correspondent account activity sufficient to determine consistency with information obtained about the type, purpose, and anticipated activity of the account.

31 C.F.R. § 103.176 ("Due Diligence Programs for Correspondent Accounts for Foreign Financial Institutions"). Significantly, pursuant to the U.S. anti-money laundering laws, the term "specified unlawful activity" includes, among other things, "fraud, or any scheme or attempt to defraud, by or ***against a foreign bank***." 18 U.S.C. § 1956(c)(7)(iii) (emphasis added).

Based on the foregoing, as part and parcel of the Agreement drafted by WFB, WFB agreed to establish a due diligence program with policies, procedures and controls that would take into account the type, purpose, and anticipated activity of the Correspondent Account to detect and prevent, among other things, fraud or any scheme to defraud against BDA, a foreign bank. *See also* 31 C.F.R. § 1010.610 (due diligence program must be part of the anti-money laundering program and must take into account the type, purpose and anticipated activity of the correspondent account.).

On July 31, 2014, consistent with WFB's obligation to comply as contract terms with the USA PATRIOT Act, Treasury regulations, and US commercial bank practices, WFB notified BDA by letter that, through its financial crimes risk management program ("Global FCRM Program"), WFB would manage financial crimes risks associated with, among other things, "Bank Secrecy Act (BSA), Anti-Money Laundering (AML), … [and] External Frauds[.]" Complaint ¶¶ 13-14; Ex. [2]. In the letter, WFB explained that its Global FCRM Program included fraud detection controls (obviously a "security program"), which included identifying unusual activity; automated transaction monitoring; customer surveillance; investigating the unusual activities identified, and determining whether they are suspicious; monitoring customer activity, and applying predictive analytics for customer-centric, cross-channel fraud detection; screening, blocking, and rejecting transactions appropriately; and reporting these matters (along with other regulatory reporting requirements). Complaint ¶¶ 13-14.

Accordingly, WFB assured BDA that it had a layered security program in place that applied "predictive analytics for customer-centric, cross-channel fraud detection," necessary to detect and deter suspicious or fraudulent activity and to report them to BDA (along with other regulatory reporting requirements), which reporting would alert BDA of such anomalous activity, and allow BDA to prevent the fraud. Complaint ¶¶ 15.[15]

In the Complaint, BDA alleged that "WFB failed to detect, block and report the Unauthorized Transfers under its Global FCRM Program." Complaint ¶ 59. As a result, BDA sufficiently alleged that "WFB failed to properly follow the security procedure, ***with the limitations in place designed to further protect BDA***." Complaint ¶ 60 (emphasis added).[16]

Consequently, section 4-A-202(2)(b) likewise prevents WFB from enforcing the Unauthorized Transfers against BDA because WFB failed to accept "the payment order[s] … in compliance with the security procedure and any written agreement … restricting acceptance of

---

[15] WFB argued that the Global FCRM Program was not part of the Agreement. WFB certainly promised in the Agreement that it would comply with the USA PATRIOT Act and Treasury regulations as contract terms, and, by letter, notified BDA that the Global FCRM Program was its way to comply with those terms and conditions of the Agreement. If the Global FCRM Program was not used to comply with the Agreement, then WFB failed to comply with its contractual obligations, and as a matter of law, would have liability under Article 4-A.

[16] WFB argues that there is nothing unusual about wire transfers outside normal operating hours of the correspondent bank. Motion at p. 14. According to WFB, funds transfer business is frequently transacted by banks outside general banking hours, citing to section 4-A-105 cmt. 2. This position highlights WFB's failure to comply with its contractual obligations. WFB's application of that comment to mean that any wire transfer issued by the sending bank outside of regular operating hours is "normal" simply highlights the failure to understand WFB's duty to apply a "customer-centric" due diligence program that takes into account the specific type, purpose, and anticipated activity of the correspondent account. BDA's correspondent account's anticipated activity did not involve issuing payment orders after BDA's normal operating hours. WFB's "customer-centric" software program must have taken that into account, as it was WFB's duty to know the anticipated activity in the account. If it did not, WFB failed to comply with its obligation under the Agreement, and thus Article 4-A, as a matter of law. The anomalous transactions were directed to new payees (***at times to the same payee from different originators***), originated during non-business hours of BDA (***a huge red flag***), and in amounts inconsistent with the customers' activity in the correspondent account.

payment orders issued in the name of the customer[.]"[17]

ii. WFB FAILED TO ACCEPT THE UNAUTHORIZED TRANSFERS IN GOOD FAITH

Section 4-A-202(2)(b) also prevents WFB from enforcing the Unauthorized Transfers against BDA because WFB failed to accept the payment orders in good faith. Complaint ¶ 61. Section 4-A-105(1)(f) defines "good faith" as "honesty in fact and the observance of reasonable commercial standards of fair dealing."

In *Experi-Metal, Inc. v. Comerica Bank*, No. 09-0-14890, 2011 WL 2433383 (E.D. Mich. June 13, 2011), the court noted that the applicable definition of good faith in Article 4-A requires both honesty in fact (a ***subjective*** standard) and observance of reasonable commercial standards of fair dealing (an ***objective*** standard). 2011 WL 2433383 at *11. The issue in the case was whether the bank acted in "observance of reasonable commercial standards of fair dealing." *Id.* Thus, "if 'reasonable commercial standards of fair dealing' obligated [the bank] to respond to the fraudulent wire transfer activity in a particular way and [the bank] failed to observe those standards, it cannot demonstrate that it acted in good faith simply by showing that it was relieved of the obligations to adhere to any of those standards in its agreement(s) with [the customer]." *Id.* at *12. The court then noted that the bank "bears the burden of demonstrating that it accepted the wire transfer payment orders in good faith." *Id.* Indeed, "to prevail, [the bank] had to present evidence conveying the reasonable commercial standards of fair dealing applicable to a bank's response to an incident like the one at issue here and to show, by a preponderance of the evidence, that its employees observed those standards in response to the criminal's phishing attack on January 22, 2009." *Id.* at *13. The court then held that the bank could not have

[17] For the same reasons, BDA stated a claim for breach of the Agreement in Count I of the Complaint.

accepted the payment orders at issue in good faith where it ignored red flags of the unauthorized transfers: "a bank dealing fairly with its customer, under these circumstances, would have detected and/or stopped the fraudulent wire activity earlier." *Id.* at *14. The court noted that those "circumstances" included the anomalous activity in the account that the bank should have detected and/or stopped, including the volume and frequency of the payment orders, the $5 million overdraft created by the fraudulent transfers in what is regularly a zero balance account, the customer's prior wire activity, and "the destinations and beneficiaries of the funds." *Id.* Specifically, the majority of funds were sent to Russia and Estonia, where "most cyber-crime is traced[.]" *Id.* at *7.

In this case, BDA alleged that "WFB failed to accept the Unauthorized Transfers in good faith because it failed to observe reasonable commercial standards of fair dealing." Complaint ¶ 61. Specifically, WFB failed to comply with reasonable commercial standards of fair dealing, as it failed to apply its fraud detection policies and procedures designed to identify unusual activity, investigate the unusual activities identified, monitor customer activity, apply predictive analytics for customer-centric, cross-channel fraud detection, and block and reject anomalous transactions. Complaint ¶¶ 13-14. WFB could not have accepted the Unauthorized Transfers in good faith where it chose to ignore red flags that would arise from anomalous activity in the Correspondent Account. Under the circumstances, WFB, in dealing fairly with BDA, under these circumstances, would have detected and/or stopped the fraudulent wire activity earlier by applying its layered security program, as it promised.

As mentioned before, the Unauthorized Transfers were made in unusual times of the day, in unusual amounts, to unusual beneficiaries in unusual geographic locations (nine of twelve, including the first four, to Hong Kong, a reputed money laundering destination), and in unusual

frequencies. In view of the various anomalies and unusual activity related to the Unauthorized Transfers, WFB's knowing and willful failure to monitor the Correspondent Account to detect, block and report to BDA the Unauthorized Transfers demonstrates a lack of good faith – willful blindness can hardly amount to "good faith." Complaint ¶ 63.

WFB mistakenly argued that to impose on it the duty to monitor incoming wires transfers to ensure that there is no anomalous activity would "impose a tremendous strain on every New York bank that processes wire transfers" and "would also defeat the efficiencies gained by using electronic funds transfers …" Motion at p. 14. These are the same old arguments rejected by Congress in enacting the USA PATRIOT Act and by the Department of the Treasury in issuing the regulations implementing the USA PATRIOT Act. The argument also flies in the face of today's banking industry standards. Indeed, BDA's position imposes no additional obligations on WFB than it already has pursuant to the federal statutes, regulations and banking industry standards included by WFB as contract terms in the Agreement.

Consequently, section 4-A-202(2)(b) also prevents WFB from enforcing the Unauthorized Transfers against BDA because WFB failed to accept the payment orders in good faith.

Accordingly, WFB is required to refund the Unauthorized Transfers because they were not authorized by BDA under section 4-A-202(1) and were not effective against BDA under section 4-A-202(2).

B. WFB IS LIABLE FOR THE UNAUTHORIZED TRANSFERS BECAUSE IT SHOULD HAVE KNOWN THAT THE PAYMENT ORDERS WERE FRAUDULENT DUE TO SUSPICIOUS ACTIVITY IN THE CORRESPONDENT ACCOUNT

Count III of the Complaint raised a claim based on the breach of the duty of care. Under New York law, as a matter of public policy, a bank owes a customer a common law duty to exercise reasonable care, which requires that a bank identify suspicious transactions and make further inquiry with the customer to verify actual authority for suspicious transactions. *Chaney v. Dreyfus Svc. Corp.*, 595 F.3d 219, 235-237 (5th Cir. 2010) (applying New York law); *Dubai Islamic Bank v. Citibank*, 126 F.Supp.2d 659, 667 (S.D.N.Y. 2000) (declining to dismiss, on a 12(b)(6) motion, a claim that the domestic bank's honoring suspicious and unauthorized transfers out of a foreign bank's correspondent account without attempting to verify actual authorization of anomalous activity constituted negligence).[18]

In *Chaney*, plaintiffs, as receivers of seven insurance companies looted by their owner through a complex fraud scheme, sued an investment company through which the owner funneled the stolen funds before moving them to his Swiss bank account. Shares purchased in the accounts of the insurance companies were subject to wire redemption instructions that appeared to direct final credit back to the account holder. *Chaney*, 595 F.3d 227. Once opened, the owner would make large stock purchases and rapid redemptions to offshore accounts via standing wire instructions. *Id.* Unfortunately, the investment company's "efforts to identify the origin, legitimacy, or ultimate destination of the funds passing through its accounts were … nonexistent." *Id.* at 227-8. The structure and speed of the transactions in the accounts "were suggestive of money laundering under the regulations promulgated by the Office of the Comptroller of the Currency, yet the "red flags" went unnoticed. *Id.* at 228.

[18] In other words, if the bank should have known that the funds were obtained illegally as a result of the red flags, it would have a duty to make further inquiry with the customer as to the suspicious transactions.

The plaintiffs claimed that the investment company was negligent in failing to uncover the owner's scheme that resulted in their losses. The district court granted summary judgment in favor of the investment company, ruling that no duty ran to the insurance companies from the investment company. On appeal, the Fifth Circuit, in applying New York law, reversed. The Fifth Circuit held that "New York law does recognize that banks and brokers owed a duty of care to their customers." *Id.* at 235 (quoting *Dubai Islamic Bank*). At a minimum, the duty of care required that the financial institution recognize the suspicious and extraordinary transactions, and verify actual authority of those suspicious transactions. *Id.* at 236-237 (citing *Collision Plan Unlimited, Inc. v. Bankers Trust Co.*, 63 N.Y.2d 827 (1984) (finding that a duty to inquire into actual authority may arise where a third party relies on apparent authority for "extraordinary" transactions)). "This duty exists apart from any contractual obligations entered into by the parties though it of course may also arise from … the parties' contractual arrangements." *Id.* at 235. Thus, the Fifth Circuit held that, under New York law, the investment company owed a duty of care arising out of the execution of the redemption orders. *Id.*

The Fifth Circuit also held that a trier of fact could reasonably conclude that the investment company was negligent in failing to verify the authenticity of the redemption orders, given the suspicious activity in the accounts. Indeed, "a jury could also reasonably find that [the investment company's] personnel, in the exercise of common judgment without any special training, should have recognized these transactions as suspicious and extraordinary[.]" *Id.* at 236. The transactions were suspicious because the orders called for funds to be transferred abroad, rather than to the domestic broker. *Id.* at 238. As a result of the suspicious activity, the investment company had a duty to make further inquire to ensure that ***actual*** authority existed.

Id. at 236-37. And, whether the investment company "breached its duty in not making some further inquiry, is a question best left for the jury." *Id.* at 237.

Similarly, in *Dubai Islamic Bank*, as in this case, a foreign bank sued a domestic bank with which it held a correspondent account, alleging millions of dollars in unauthorized transfers. The terms of the contract consisted of, among other things, the foreign bank's agreement to pay correspondent fees, and the domestic bank's agreement to service the correspondent account, perform transactions authorized by the foreign bank, and safeguard the correspondent account by enforcing money laundering and the domestic bank's so-called "know your customer" rules. *Dubai Islamic Bank*, 126 F. Supp. 2d at 662. As part of its advertised "know your customer" policy, the domestic bank represented that it prepared a financial profile for each new customer, and that, among other things, such profile preparation verified the customer's financial history and source of wealth. *Id.* The domestic bank also represented that it would undertake due diligence, including understanding the types of transactions the customer would typically conduct. *Id.*

Beginning in our about November 28, 1995, and continuing for about two years, tens of millions of dollars were debited by the domestic bank from the foreign bank's correspondent account without proper authorization, and the proceeds were credited to numerous locations around the world through a series of financial transactions. *Id.* at 663. None of the debits were properly authorized by the foreign bank's Board of Directors and were contrary to the foreign bank's interests. *Id.* The domestic bank failed to take ***any*** action to prevent or stop the debiting of funds from the correspondent account and crediting the accounts of the fraudsters, despite the suspicious nature of the activity. *Id.* at 663. As a result, the foreign bank sued the domestic bank for, among other things, negligence, breach of contract and violation of Article 4-A.

In the lawsuit, the domestic bank moved to dismiss, arguing that the foreign bank could not bring a negligence claim. *Id.* at 667. In response, the foreign bank argued that "a bank is not immune from common law liability arising from its tortious conduct simply because wire transfers may be involved." *Id.* at 666. The district court agreed with the foreign bank, ruling that "[c]ourts have stated that banks owe a duty of care to their customers." *Id.* at 667. The domestic bank had a duty to exercise reasonable skill and care in carrying out its activities for its customer. *Id.* (citing *Bank of Brussels Lambert, S.A. v. Intermetals Corporation*, 779 F. Supp. 742, 747 (S.D.N.Y. 1991)). Accordingly, the domestic bank could be liable in tort for negligence based on unauthorized and suspicious transfers of funds from the correspondent account of the foreign bank, and the bank's failure to notify the foreign bank of the suspicious activity. *See also 2006 Frank Calandra, Jr. Irrevocable Trust v. Signature Bank Corp.*, 11–4090, 2012 WL 5861802 *2 (2nd Cir. Nov. 20, 2012) ("It is true, as Plaintiffs point out, that a bank has a duty to make reasonable inquiries to prevent fraud where it has '***notice*** or knowledge that a diversion is intended or being executed.'") (emphasis added).

Thus, *Chaney* and *Dubai Islamic Bank* stand for the following propositions:

(1) Under New York law, as a matter of public policy, a bank owes a customer a common law duty to exercise reasonable care;

(2) The duty of care requires that the bank recognize suspicious or extraordinary transactions (i.e., the bank should have known of the fraudulent nature of the payment orders due to their anomalous characteristics);

(3) The duty of care includes the duty to make further inquiry with the customer to ensure that actual authority exists (only) for suspicious or

extraordinary transactions; and

(4) The duty of care is independent of any contract between the bank and the customer, though it of course may also arise from the parties' contractual arrangements[19];

In applying the foregoing rules of law, it cannot be seriously disputed that BDA stated a claim for negligence against WFB.

First, BDA was a customer of WFB. Accordingly, WFB owed BDA a common law duty to exercise reasonable care. The duty of care required that WFB recognize the suspicious and extraordinary transactions, and make further inquiry with BDA regarding the suspicious transactions.

Second, BDA alleged that the unauthorized payment orders spanning a mere nine (9) days were suspicious, unusual or anomalous in that they were (i) made at unusual times of the day for the SWIFTs (given that all were outside normal operating hours of BDA's for sending payment orders), (ii) in unusual amounts given the historic activity in the account, (iii) made to unusual beneficiaries in unusual geographic locations (nine of the twelve transfers were to beneficiaries located in Hong Kong, a reputed money laundering hub), (iv) made with unusual frequency (twelve in nine days, with the second, third and fourth transfers being made to the same entity in Hong Kong within the span of a mere 26 hours for substantial amounts of money), and (v) characterized by having the same beneficiary at times receiving substantial amounts of

[19] Paragraph 2.3 of the Agreement actually contemplated that BDA could hold WFB liable for breach of the duty to exercise ordinary care:

> [I]f Correspondent is able to show that Wells Fargo failed to exercise ordinary care in paying any unauthorized transaction and that Wells Fargo's failure directly and substantially contributed to the loss, the parties agree that the loss will be allocated between Wells Fargo and Correspondent based on the extent to which Wells Fargo's failure to exercise ordinary care contributed to the loss.

money from multiple customers of BDA (e.g., Regal Prosper Trading Limited receiving funds from three different customers of BDA). BDA alleges that despite these numerous anomalies, WFB failed to monitor the Correspondent Account to detect and alert BDA of the suspicious activity.

Consequently, BDA properly alleged that, under the circumstances, WFB violated its duty of care by negligently honoring the unauthorized transfers, and thereby negligently failing to properly monitor the correspondent account for suspicious activity, failing to screen, block and reject the Unauthorized Transfers, and/or failing to report the Unauthorized Transfers in a timely manner to BDA.

Third, BDA further alleges that an inquiry would have revealed the scheme by outsiders and averted the losses resulting from the unauthorized transfers, as BDA would have verified that any and all of the transactions were unauthorized.

The foregoing clearly and unequivocally shows that BDA stated a claim under New York law for negligence against WFB.

C. ARTICLE 4-A PREEMPTS NEITHER THE NEGLIGENCE CLAIM NOR THE BREACH OF CONTRACT CLAIM

WFB mistakenly argued that Article 4-A precludes a claim for negligence and breach of contract. "Clearly, parties whose conflict arises out of a funds transfer should look first and foremost to Article 4–A for guidance in bringing and resolving their claims, but the article has not completely eclipsed the applicability of common law in the area." *Sheerbonnet, Ltd. v. American Exp. Bank, Ltd.*, 951 F. Supp. 403, 407 (S.D.N.Y. 1995). "The exclusivity of Article 4–A is deliberately restricted to 'any situation covered by particular provisions of the Article.'" *Id.* at 407-8. "Conversely, situations not covered are not the exclusive province of the Article." *Id.* at 408. Indeed, "[c]ommentators uniformly recognize that Article 4–A is not a hermetic legal

seal over funds transfers." *Id.* (citing to *J.J. White & R.S. Summers, Uniform Commercial Code, § 1–2*, at p. 132 (1993 pocket part) ("With the adoption of Article 4A, electronic funds transactions are governed not only by Article 4A, but also common law, contract, Federal Reserve rules, Federal Reserve operating letters, rules of automated clearing houses, CHIPS and Title IX of the Federal Consumer Credit Protection Act.")). Thus, "Article 4–A of the New York Uniform Commercial Code is ***not*** the exclusive means by which a plaintiff can seek to redress an alleged harm arising from a funds transfer." *Id.* at 409 (emphasis added). "The rules of [Article 4-A] are transactional, aimed essentially at resolving conflicts created by erroneous instruction or execution of payment orders, whether by the originator, by an intermediary or receiving bank, or by the beneficiary's bank." *Id.* at 412.

Consistent with *Sheerbonnet, Ltd.*, the court in *Regions Bank v. Provident Bank, Inc.*, 345 F.3d 1267 (11th Cir. 2003), held that:

> Article 4A is silent with regard to claims based on the theory that the beneficiary bank accepted funds when it knew or should have known that the funds were fraudulently obtained. Therefore, a provision of state law that requires a receiving or beneficiary bank to disgorge funds that it knew or should have known were obtained illegally when it accepted a wire transfer is not inconsistent with the goals or provisions of Article 4A.
>
> ***
>
> Interpreting Article 4A in a manner that would allow a beneficiary bank to accept funds when it knows or should know that they were fraudulently obtained, would allow banks to use Article 4A as a shield for fraudulent activity. It could hardly have been the intent of the drafters to enable a party to succeed in engaging in fraudulent activity, so long as it complied with the provisions of Article 4A.

345 F.3d at 1275-6. Thus, Article 4-A is silent with regard to claims based on the theory that the receiving bank accepted funds when it ***should have known***, based on red flags, that the funds were fraudulently obtained. *Id.* Thus, a duty by the receiving bank to refunds monies that it should have known were obtained illegally when it accepted a wire transfer is not inconsistent

with the goals or provisions of Article 4-A. *Id.*

In *Ma v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, 597 F.3d 84 (2d Cir. 2010), the Second Circuit agreed with the Eleventh Circuit in *Regions Bank*. 597 F.3d at 89 (holding that "[n]ot all common law claims are per se inconsistent with [Article 4-A's] regime." citing *Regions Bank* and *Sheerbonnet, Ltd.*). However, the Second Circuit in that case held that the plaintiff's common law claims were inconsistent with Article 4-A because they simply based liability on the bare "assertions that he did not order or approve any of the disputed electronic transfers of funds from his accounts[.]" *Id.* at 90.[20]

BDA's negligence claim is based neither on the bare assertion that BDA did not order or authorize the Unauthorized Transfers, nor on the bare assertion that WFB simply failed to properly follow the SWIFT Authentication procedure. Instead, the claim, which the Agreement drafted by WFB contemplates, is based on the negligent failure to detect and investigate suspicious activity on the account based on several anomalous characteristics of the payment orders. In other words, it is based on the fact that WFB should have known that the funds were fraudulently obtained. Interpreting Article 4-A in a manner that would allow WFB to accept the payment orders as the receiving bank when it should have known that they were fraudulently obtained would allow banks to use Article 4-A as a shield for willfully blinding themselves to the fraudulent activity.

Likewise, Article 4-A does not preempt BDA's contractual claim. At its core, the contract

[20] WFB reliance on *ReAmerica S.A. v. Wells Fargo Bank Intern.*, 577 F.3d 102 (2d Cir. 2009), is misplaced, as it was decided under Minnesota law. Likewise, WFB erroneously relies on the case of *Grain Traders, Inc. v. Citibank, N.A.*, 160 F.3d 97 (2d Cir. 1998), which is inapplicable because it involved a lawsuit brought by a ***non-customer*** of the ***intermediary*** bank that was sued. *Grain Traders, Inc.* is not applicable to a situation involving a ***customer*** who sues the bank and in effect claims that the bank should have known that the funds were fraudulently obtained.

claim, as the negligence claim, is based on the failure of WFB to detect, investigate, and reject or block suspicious transactions in the Correspondent Account. In fact, BDA alleges that "WFB materially breached its contractual duties by failing to detect, block and report the Unauthorized Transfers." Complaint ¶ 44. However, these duties stem, not from public policy, but from WFB's promise to comply, as contract terms, with the USA PATRIOT Act, the regulations of the Treasury Department, and general US commercial banking practices. In fact, the contractual duties are even broader that the tort duties, as they included the duties to identify unusual activity, have automated transaction monitoring, investigate the unusual activities identified, monitor customer activity, apply predictive analytics for customer-centric, cross-channel fraud detection, and screen, block, and reject transactions appropriately. A common law claim for breach of contract that imposes higher standards on the bank is "not inherently inconsistent" with an Article 4-A claim. *Patco Const. Co., Inc.*, 684 F.3d at 215.[21]

Thus, based on these duties, WFB should have known of the fraudulent nature of the payment orders as a result of the numerous red flags. It had a contractual duty to detect, investigate and block (or reject) the Unauthorized Transfers. This it failed to do. Thus, Article 4-A does not preempt the breach of contract claim.

The case relied upon by WFB, *2006 Frank Calandra, Jr. Irrevocable Trust v. Signature Bank Corp.*, 816 F. Supp. 2d 222 (S.D.N.Y. 2011), is inapplicable. As in *Ma*, the breach of contract claim relied on the bare assertion that the bank failed to perform investigative steps before and after carrying out wire transfers. 816 F.Supp. 2d at 237. However, nowhere was there

[21] WFB argued in its Motion at p. 21 that section 4-A-202(6) provides that "'rights and obligations arising under [Section 4-A-202)] or Section 4-A-203 may not be varied by Agreement.'" The problem is that WFB omits other relevant language in the statute, to wit: "Except as provided in this section [Section 4-A-202] …". Section 4-A-202(2)(b) clearly allows the customer and the bank to create additional contractual obligations that restrict acceptance of payment orders. That is exactly what happened in this case.

any discussion that the agreement with the bank provided for such an obligation or other higher obligations. Moreover, as in *Ma*, but unlike *Regions Bank* and *Sheerbonnet, Ltd.*, the claim was not based on the fact that the bank knew or should have known of the fraudulent nature of the payment orders as a result of numerous red flags.

Thus, neither the negligence claim nor the breach-of-contract claim is preempted.

D. THE AGREEMENT DOES NOT PROHIBIT ANY CLAIM FOR NEGLIGENCE

WFB argued that the Agreement prohibits any negligence claim. Motion at p. 22. According to WFB, "[t]he Agreement states that 'Wells Fargo's liability, if any, will be *limited* to those actual damages which are the direct result of Wells Fargo's *gross negligence* or *willful misconduct*." *Id.* (citing to paragraph 7.15 of the Agreement) (emphasis in the original).

The problem with WFB's argument is that the sentence quoted by WFB actually begins with the words: "Unless otherwise provided in these Terms & Conditions …" Agreement ¶ 7.15. And, paragraph 2.3 of the Agreement drafted by WFB expressly states that:

> [I]f Correspondent is able to show that Wells Fargo failed to exercise ordinary care in paying any unauthorized transaction and that Wells Fargo's failure directly and substantially contributed to the loss, the parties agree that the loss will be allocated between Wells Fargo and Correspondent based on the extent to which Wells Fargo's failure to exercise ordinary care contributed to the loss.

As to WFB's "paying any unauthorized transaction," WFB can be held liable for failing to exercise ordinary care, as expressly stated in the Agreement. Accordingly, WFB's reliance on paragraph 7.15 is misplaced. The Agreement does not prohibit the negligence claim.

III. CONCLUSION

WFB's Motion should be denied. BDA's has stated claims for breaches of Article 4-A, the Agreement, and the duty of care. Article 4-A does not preempt any of the common law claims. Finally, the Agreement does not prohibit the negligence claims. Accordingly, BDA

respectfully requests that this Court deny WFB's motion to dismiss, and to grant such further relief as this Court deems just and proper.

Respectfully submitted,

WNF LAW, P.L. - Waserstein Nunez & Foodman
Attorneys for Plaintiff Banco Del Austro, S.A.
1111 Brickell Avenue Suite 2200
Miami, Florida 33131
Phone: (305) 760-8500 / Fax: (305) 760-8510

By: */s/ John G. Marfoe*
Carlos Nunez-Vivas (*pro hac vice)*
can@wnflaw.com
Daniel Foodman (*pro hac vice)*
df@wnflaw.com
John G. Marfoe (*pro hac vice)*
jgm@wnflaw.com

CERTIFICATE OF SERVICE

I certify that on March 31, 2016, this document was served by transmission of a Notice of Filing generated by CM/ECF upon the following:

Jeffrey J. Chapman (jchapman@mcguirewoods.com)
Aaron F. Jaroff (ajaroff@mcguirewoods.com)
McGuireWoods, L.L.P.
1345 Avenue of the Americas, 7th Floor
New York, New York 10105-0106
(212) 548-2100
Attorneys for Defendant Wells Fargo Bank, N.A.

/s/ John Marfoe